

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP04/014099

International filing date: 10 December 2004 (10.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: EP  
Number: PCT/EP04/004923  
Filing date: 07 May 2004 (07.05.2004)

Date of receipt at the International Bureau: 11 February 2005 (11.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse



**Bescheinigung**

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten internationalen Patentanmeldung überein.

**Certificate**

The attached documents are exact copies of the international patent application described on the following page, as originally filed.

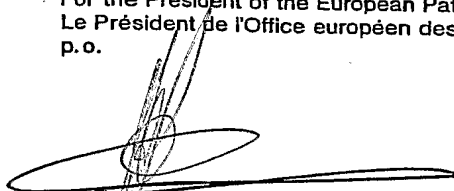
**Attestation**

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet international spécifiée à la page suivante.

Den Haag, den  
The Hague,  
La Haye, le

10 FEB. 2005

Der Präsident des Europäischen Patentamts  
Im Auftrag  
For the President of the European Patent Office  
Le Président de l'Office européen des brevets  
p.o.



Y. Marinus-v.d. Nieuweland

Patentanmeldung Nr.  
Patent application no.  
Demande de brevet n°

PCT/EP 04/004923



**Blatt 2 der Bescheinigung**  
**Sheet 2 of the certificate**  
**Page 2 de l'attestation**

---

**Anmeldung Nr.:**  
**Application no.:**  
**Demande n°:** PCT/EP 04/004923

**Anmelder:**  
**Applicant(s):**  
**Demandeur(s):**

1. TELECOM ITALIA S.p.A. - Milano, Italy
2. BALTATU, Madalina - Torino, Italy (US only)
3. D'ALESSANDRO, Rosalia - Torino, Italy (US only)

**Bezeichnung der Erfindung:**  
**Title of the invention:**  
**Titre de l'invention:** User authentication method based on the utilization of biometric identification techniques and related architecture

**Anmeldetag:**  
**Date of filing:**  
**Date de dépôt:** 07 May 2004 (07.05.2004)

**In Anspruch genommene Priorität(en)**  
**Priority(ies) claimed**  
**Priorité(s) revendiquée(s)**

**Staat:**  
**State:**  
**Pays:**

**Tag:**  
**Date:**  
**Date:**

**Aktenzeichen:**  
**File no.**  
**Numéro de dépôt:**

**Bemerkungen:**  
**Remarks:**  
**Remarques:**

**Further Applicants:**

4. D'AMICO, Roberta - Torino, Italy (US only)



TEL0903

1

USER AUTHENTICATION METHOD BASED ON THE UTILIZATION OF  
BIOMETRIC IDENTIFICATION TECHNIQUES AND RELATED  
ARCHITECTURE

\* \* \* \* \*

5 The present invention refers in general to the  
field of secure authentication system. More  
particularly, the present invention refers to a user  
authentication method based on the utilization of  
biometric identification techniques and related  
10 architecture.

Authentication is the process by which an entity,  
such as a financial institution, a bank, etc.,  
identifies and verifies its customers or users to  
itself and identifies and verifies itself to its  
15 customers or users.

Authentication includes the use of physical  
objects, such as cards and/or keys, shared secrets,  
such as Personal Identification Numbers (PIN's) and/or  
passwords, and biometric technologies such as voice  
20 prints, photos, signatures and/or fingerprints.  
Biometric tasks include, for example, an identification  
task and a verification task. The verification task  
determines whether or not the person claiming an  
identity is really the person whose identity has been  
25 claimed.

The identification task determines whether the  
biometric signal, such as a fingerprint, matches that  
of someone already enrolled in the system.

Various biometrics have been considered for use  
30 with smart cards, such as fingerprints, hand prints,  
voice prints, retinal images, handwriting samples and  
the like.



TEL0903

2

An example of a biometric-based smart card is shown in US-A-5,280,527 describing a credit card sized token (referred to as biometric security apparatus) containing a microchip, in which a sample of the authorised user's voice is stored. In order to gain access to an account, the user must insert the token into a designated slot of an ATM, and then speak with the ATM. If a match is found between the user's voice and the sample enrolment of the voice stored into the microchip, access to the account is granted.

Although the system disclosed in US-A-5,280,527 reduces the risks of unauthorised access, if compared with conventional PIN-based systems, however, to the extent that the credit card and the microchip disposed therein can be tampered with, the system does not provide the level of reliability and security that is often required in nowadays finance transactions.

In WO-A-0139134 a security system is further disclosed, comprising: a central unit with a biometric sensor to detect biometric data representing characteristic biometric features of a person; at least one portable data carrier; a memory means for storing biometric reference data representing the biometric reference features of the person in the system; a control system capable of generating an authorisation signal to control a functional unit depending on a comparison between the biometric data detected by the sensor and the reference data.

In the security system proposed in such document, the reference data, that are compared with the biometric data detected by the sensor to ascertain the authenticity of the user, are not wholly stored into





TEL0903

3

the data carrier, in the conventional manner, but are splitted, partly in the data carrier and partly in the reading device. Only the combination of data carrier and reading device will produce the complete  
5 information needed for authentication.

The invention is particularly advantageous if the biometric sensor is a fingerprint sensor. A fingerprint sensor determines the locally resolved position of minutiae of the fingerprint. The minutiae are singular  
10 points of the papillary lines of a fingerprint. These might be end points, branches or similar points of the papillary lines of the fingerprint. The local position is determined depending on the distance from a reference point or radius to the angle related to a  
15 reference direction.

In order to personalise the data carrier, the fingerprint of the data carrier owner is reproduced and appropriate reference values are determined for radius and angle. These values are then stored into the  
20 system. For practical purpose, the radius reference data are stored only on the data carrier and the angle reference data are stored only on the reading device. Alternatively, the angle reference data are stored in the data carrier and the distance reference data are  
25 stored on the reading device.

The Applicant faced the problem of realising a method for authenticating users based on the use of biometric identification techniques, that is secure, independent from the used biometric identification  
30 techniques and that protects user privacy.

The Applicant has observed that the above-described problem can be solved by a user



TEL0903

4

authentication method based on the use of biometric identification techniques comprising the steps of: generating a reference biometric template from a first biometric image of a user to be authenticated and, 5 afterwards, splitting the reference biometric template into a first and a second reference biometric template portion, said first and second reference biometric template portion being separable. The first and the second biometric reference template portion are then 10 signed, enciphered and stored in different memories.

More specifically, a user authentication method based on the use of biometric identification techniques comprises an enrolment step and a verification step, said enrolment step including the steps of:

- 15 - generating a reference biometric template from a first biometric image of a user to be authenticated;
- splitting said reference biometric template into a first and a second reference biometric template portion;
- 20 - enciphering said first and second reference biometric template portion; and
- storing each one of said reference biometric template portions into a different memory.

Another aspect of the present invention refers to 25 an architecture based on the use of biometric identification techniques comprising:

- at least one data enrolment system for generating a reference biometric template from a first biometric image of a user to be authenticated, said 30 data enrolment system comprising a Host Computer for splitting said reference biometric template into a first and a second reference biometric template portion



TEL0903

5

that are physically separable and for enciphering said first and second reference biometric template portion;

- at least one portable data carrier associated with said user to be authenticated, said data carrier comprising a memory for storing said first signed and enciphered reference biometric template portion; and

- at least one data verification system comprising a memory for storing said second signed and enciphered reference biometric template portion.

10 Another aspect of the present invention refers to a portable data carrier associated with a user that has to be authenticated through a user authentication architecture, said data carrier including a microprocessor comprising a memory for storing a first  
15 reference biometric template portion associated with said user to be authenticated, said first reference biometric template portion being signed and enciphered, said portable data carrier being adapted to received as input, from said user authentication architecture, a  
20 second reference biometric template portion and a live template associated with said user to be authenticated, said second reference biometric template portion and said live template being signed and enciphered, said microprocessor further comprising:

25 - a processing logic for deciphering said first and second reference biometric template portion and for recomposing therefrom said reference biometric template associated with said user to be authenticated;

- a comparing logic for comparing said reference  
30 biometric template recomposed with said live template and sending a result of said comparison to said user authentication architecture.



TEL0903

6

Another aspect of the present invention refers to a data verification system comprising an electronic device and a portable data carrier associated with a user that has to be authenticated, said data carrier  
5 being adapted to store a first reference biometric template portion associated with a user to be authenticated, said first reference biometric template portion being signed and enciphered;

said electronic device comprising:

10 - a memory adapted to store a second reference biometric template portion associated with a user to be authenticated, complementary with said first portion, said second reference biometric template portion being signed and enciphered;

15 - an image acquiring and processing device for generating a live template ;

said electronic device being adapted to encipher and sign said live template , transmit said second reference biometric template portion and said live  
20 template to said portable data carrier and authenticate said user depending on the result of a comparison performed by said data carrier between said live template and a reference biometric template of said user to be authenticated, said reference biometric  
25 template being recomposed by using said first and second reference biometric template portion.

A further aspect of the present invention deals with a computer program product that can be loaded in the memory of at least one electronic processor and  
30 comprising portions of software code to perform the process according to the invention when the product is executed on a processor: in this context such diction





TEL0903

7

must be deemed equivalent to the mention of a means readable by a computer comprising instructions to control a network of computers in order to perform a process according to the invention. The reference to  
5 "at least one electronic processor" is obviously aimed to point out the possibility of carrying out the solution according to the invention in a de-centralised context.

Further preferred aspects of the present invention  
10 are disclosed in the dependent claims and in the present description.

The features and the advantages of the present invention will result from the herein below description of an embodiment, provided as a non-limiting example,  
15 with reference to the enclosed drawings, in which:

- figure 1 is a schematic representation of a user authentication architecture according to the invention;

- figure 2 shows a flow diagram related to implementing a first step of a user authentication  
20 method according to the invention; and

- figure 3 shows a flow diagram related to implementing a second step of the user authentication method according to the invention.

With reference to figure 1, the user  
25 authentication method according to the invention is applied to a user authentication architecture 1 comprising a data enrolment system 2, a data verification system 3 and a portable data carrier 4, this latter one belonging to a user that has to be  
30 authenticated. The data carrier 4 can be a substrate whose sizes are substantially rectangular, such as for example an access card, a credit card, a debit card, an



8

identification card, a smart card, a SIM card. The data carrier 4 is equipped with a microprocessor 5 including a processing logic 5a, a comparing logic 5b and a memory 6.

5 Always with reference to figure 1, in a preferred embodiment, the data enrolment system 2 comprises a Host Computer 7, for example a personal computer, a business computer, etc., having enough memory 7a to store biometric data of a user that has to be  
10 authenticated. The data enrolment system 2 can also include an image acquiring and processing device 8, connected to the Host Computer 7, and a data reading/writing device 60, also connected to the Host Computer 7 realising the interface with the data  
15 carrier 4. The data reading/writing device 60 can be, for example, a smart card reader, if the data carrier 4 is a smart card, or a cellular phone, if the data carrier 4 is a SIM card.

Specifically, the image acquiring and processing  
20 device 8 includes: a sensor 9 of the biometric type, for example a television camera, to detect a first biometric image (i.e., biometric data sample) of the user that has to be authenticated, for example a face template; an image processor 10, connected between  
25 sensor 9 and Host Computer 7, to generate a reference biometric template from the user biometric image, detected through sensor 9.

Preferably, the data enrolment system 2 is a separated system from the data verification system 3  
30 and is placed in a secure environment.

In a preferred embodiment, the data verification system 3 comprises an electronic device 11, for example



TEL0903

9

a personal computer, a palmtop computer, a cellular telephone, an hand-held PC, a smart-phone, having enough memory 11a to store biometric data of a user that has to be authenticated.

5       The data verification system 3 can also comprise: a data base, of a known type and therefore not shown in figure 1, managed by a remote system connected to the electronic device 11; an image acquiring and processing device 12; a data reading/writing device 61 realising  
10 the interface with the data carrier 4. The image acquiring and processing device 12 and the data reading/writing device 61 are both connected to the electronic device 11. Moreover, the data reading/writing device 61 can be, for example, a smart  
15 card reader, if the data carrier 4 is a smart card, or a cellular phone, if the data carrier 4 is a SIM card.

Specifically, the image acquiring and processing device 12 comprises: a sensor 13, of the biometric type, for example a television camera, to detect a  
20 second biometric image (the face template) of the user that has to be authenticated. The image acquiring and processing device 12 also includes an image processor 14, connected between sensor 13 and electronic device 11, to generate a live template from the user biometric  
25 image detected through the sensor 13. The electronic device 11 can also comprise a processing logic (not shown in figure 1) able to read and interpret the comparison operation result between reference biometric template and live template performed by the data  
30 carrier 4, as will be described more in detail below.

It is to be remarked that, in the following description, for enciphering and deciphering biometric



TEL0903

10

data, cryptographic algorithms of the asymmetrical type, for example the RSA algorithm, are preferably used. In particular, these algorithms are based on the use of two different keys in the data enciphering and  
5 deciphering steps and on the existence of a PKI (Public Key Infrastructure), for example based on standard X.509 described in R. Housley, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, 1999.

10 The user authentication method, according to the invention, will now be described with reference to the flow diagrams shown in figures 2-3.

In a preferred embodiment, the method according to the invention comprises an enrolment step 20, performed  
15 by the data enrolment system 2 and shown in figure 2, and a verification step 40, performed by the data verification system 3 and the data carrier 4 and shown in figure 3.

With reference to figure 2, initially the  
20 enrolment step 20 provides an initialisation step 21 of the data enrolment system 2, of the data verification system 3 and the data carrier 4.

Specifically, the initialisation step 21 provides:

- storing, in the memory 7a of Host Computer 7, a  
25 pair of public  $KE_{pub}$  and private  $KE_{pr}$  keys associated with the data enrolment system 2, the related digital certificate  $C_e$  containing the public key  $KE_{pub}$  signed with the private key issued by a secure Certification Authority and, possibly, the digital certificate  $C_{Ac}$  of  
30 the same Certification Authority;

- storing, in the memory 6 of data carrier 4, a pair of public  $KU_{pub}$  and private  $KU_{pr}$  keys associated





TEL0903

11

with the user to be authenticated, the related digital certificate  $C_v$  containing the public key  $KU_{pub}$  signed with the private key of the secure Certification Authority and, possibly, the digital certificate  $C_{ac}$  of the same Certification Authority. Alternatively, the data carrier 4 initialisation can provide for the generation of the pair of public and private keys  $KU_{pub}$ ,  $KU_{pr}$  aboard the data carrier 4 itself (on-card) and the transmission of the certification request for the public key  $KU_{pub}$  to the secure Certification Authority. The initialisation process is then finalised by installing the user digital certificate  $C_v$  on the data carrier 4 and distributing the related certificate to the data enrolment system 2 and the data verification system 3. All these operations can be performed in the microprocessor 5; and

- storing, in the memory 11a of electronic device 11, a file containing a pair of public  $KV_{pub}$  and private  $KV_{pr}$  keys associated with the data verification system 3, the related digital certificate  $C_v$  containing the public key  $KV_{pub}$  signed with the private key issued by the secure Certification Authority and, possibly, the digital certificate  $C_{ac}$  of the same Certification Authority.

The enrolment step 20 then proceeds with detecting, through the sensor 9, a first biometric image of the user to be authenticated (block 22). Afterwards, the first biometric image is transferred to the image processor 10 that generates the reference biometric template (block 23).

The reference biometric template is then stored into the memory 7a of the Host Computer 7 (block 24).



TEL0903

12

Afterwards, the Host Computer 7 decomposes the reference biometric template into a first and a second reference biometric template portion (block 25), using a splitting algorithm that will be described more in detail herein below, and then destroys the original copy of the reference biometric template (block 26).

At this time, the Host Computer 7 signs the first and the second reference biometric template portion with the private key  $KE_{pr}$  of the data enrolment system 2 (block 27) and then enciphers the two portions with the public key  $KU_{pub}$  of the user to be authenticated (block 28).

Afterwards, the Host Computer 7 transfers the first reference biometric template portion onto the data carrier 4 (block 29). Here, the first reference biometric template portion is stored into a protected area 6a (shown in figure 1) of the memory 6 (block 30). For example, the memory 6a area can be protected through PIN.

Communication between data enrolment system 2 and data carrier 4 can occur for example through the communication protocol implemented in the reading/writing device 60. The reading/writing device 60 is also equipped with a logic (an application program) that checks the data transfer.

The second reference biometric template portion is instead transferred and stored into the memory 11a of the electronic device 11 (block 31).

Alternatively, the second reference biometric template portion can be transferred and stored into the data base.



TEL0903

13

The transfer of the second reference biometric template portion from data enrolment system 2 to electronic device 11, or to data base, can occur by using methods of the OOB ("Out Of Band") type. In particular, these methods assume that data are not transferred in a network, but are transferred using alternative communication channels, such as, for example, a telephone channel or the traditional mail.

Less preferably, the transfer of the second reference biometric template portion can occur through a modem or a communication network, for example a TCP/IP or GSM network.

With reference now to figure 3, the verification step 40 starts when a user, by entering the data carrier 4 into the data reading/writing device 61, asks the user architecture 1 to be authenticated (block 40a). Under these conditions, the data verification system 3, through the sensor 13, detects a second biometric image of the user that has to be authenticated (block 41). This second biometric image is then transferred to the image processor 14 that generates the live template (block 42). Afterwards, the live template is sent to the electronic device 11 that signs it with the private key  $KV_{pr}$  of the data verification system 3 and enciphers it with the public key of the user  $KU_{pub}$  (block 43).

At that time, the electronic device 11, through the reading/writing device 61, transmits to the data carrier 4 both the live template and the second reference biometric template portion, this latter one stored locally or recovered by the data base, enclosing a univocal Nonce (namely an aleatory value, used a



TEL0903

14

single time in a cryptographic scheme) to guarantee the authenticity of the current data verification session (block 44). The univocal Nonce is also enciphered and signed. Such operation guarantees for example the  
5 protection from the so-called replay attacks (attacks where the attacking person is an authorised user that re-proposes to the system, in a following authentication session, a previously positive authentication session as regards the interested user).

10 Communication between data verification system 3 and data carrier 4 can occur for example through the communication protocol implemented in the reading/writing device 61. The reading/writing device 61 is also equipped with a logic (an application  
15 program) that checks the data transfer.

Afterwards, the data carrier 4, using its own private key  $KU_{pr}$ , deciphers the second reference biometric template portion and checks its signature by using the public key  $KE_{pub}$  of the data enrolment system  
20 2 (block 45). In case of check success, the data carrier 4, through a recombination algorithm, stored into the memory 6 and shown below, recomposes the reference biometric template (block 46) using the now deciphered second reference biometric template portion  
25 and the first reference biometric template portion, stored into the protected memory area 6a.

Afterwards, the data carrier 4, using its own private key  $KU_{pr}$ , deciphers the live template transmitted by the data verification system 3 and  
30 checks its signature by using the public key  $KV_{pub}$  of the data verification system 3 (block 47).





TEL0903

15

If all previously-described check operations realised through the processing logic 5a of the microprocessor 5, have a positive result, the data carrier 4 performs a comparison operation between the reference biometric template and the live template (block 48).

Preferably, the comparison operation is performed by the comparing logic 5b of the microprocessor 5 as an atomic operation using known comparison functions depending on the biometric identification techniques used. For example, for the face template, as comparison functions, those provided in the Principal Component Analysis (Eigenfaces) or Local Features Analysis, or Neural Networks or 3D or wavelet Gabor, etc. techniques can be used.

Afterwards, the data carrier 4 transfers to the data verification system 3 the comparison operation result together with the univocal Nonce previously received by the data verification system itself (block 49).

The comparison operation result and the univocal Nonce can for example be sent as a message signed with the user private key  $K_{u_{pr}}$  and enciphered with the public key  $KV_{pub}$  of the data verification system 3.

At this time, the electronic device 11, using the private key  $KV_{pr}$  of the data verification system 3, deciphers the message sent thereto by the data carrier 4, checks its signature, and, depending on the comparison operation result, grants or not the user access to the required service (block 50).

In case a data base is used for storing the second reference biometric template portion, it is necessary



TEL0903

16

to make secure also the communication between electronic device 11 and remote data base managing system. This can be obtained by using, for example, the previously-described authentication, privacy and non-  
5 repudiation cryptographic mechanisms, in order to guarantee the authentication of affected parts, in addition to integrity and privacy of transferred data.

Moreover, the remote data base managing system can use access control methods, of the Access Control List  
10 type (with user authentication through userID and Password or through digital certificates) to guarantee a secure access to data contained in the data base.

Preferably, the splitting algorithm used by the data enrolment system 2 to split the reference  
15 biometric template into the two portions of reference biometric template, is a secret splitting algorithm, that can be used in the cryptographic techniques of the "secret sharing scheme" type. In this case a secret is divided into N parts, securely transferred to N  
20 entities with the property that, starting from a single part of the secret, the original cannot be rebuilt. An algorithm of this type is for example described in H. Feistel in "Cryptographic Coding for Data-Banking Privacy", IBM Research, New York, 1970.

25 More in detail, the splitting algorithm comprises an enrolment step in which the data enrolment system 2 that created the template t (the reference biometric template) generates a random number  $t_1$  (the first reference biometric template portion) of the same size  
30 (length) of the template t. Afterwards the data enrolment system 2 applies a XOR function to t and  $t_1$  to



17

generate a value  $t_2$  (the second reference biometric template portion), namely:

$$t \text{ XOR } t_1 = t_2$$

$t_1$  is then stored in a protected mode (that provides for signature and enciphering) on the data carrier 4 while  $t_2$  is stored in a protected mode (that provides for signature and enciphering) on the data verification system 3 or in the central data base.

The recombination algorithm for the template  $t$ , used by the data carrier 4 to recompose the template  $t$  from  $t_1$  and  $t_2$ , is, mathematically, the reverse function of the previously-described splitting algorithm. In particular, the data carrier 4, after having obtained  $t_2$ , performs the XOR between  $t_1$  and  $t_2$  rebuilding the original value of the template  $t$ , namely:

$$t_1 \text{ XOR } t_2 = t.$$

If all described operations are correctly performed, the technique is secure since by possessing a single part,  $t_1$  or  $t_2$ , it is not possible to obtain the template  $t$ .

The advantages that can be obtained with the described user authentication method are as follows.

Firstly, the user authentication method is secure since an hacker that tries to violate either the data carrier 4 or the data verification system 3 does not obtain enough elements to go back to the reference biometric template, since this latter one is partly stored in the data carrier 4 and partly in the data verification system 3. In this way, both user privacy compliance, and the chance of using the same biometric technique also in case of violation/corruption of only one part of the reference biometric template, are



guaranteed. In fact, the reference biometric template is a piece of information depending on the used biometric technique: by applying the same biometric technique to the image of the same person, a reference  
5 biometric template is obtained that is very similar to the original one. Therefore, if the whole reference biometric template falls in the hand of an hacker, this latter one could use it for disguising as the user enabled to the service, impairing the used biometric  
10 technique. Moreover, it is plausible that, through a reverse-engineering process, the hacker can go back to the mode used by the biometric technique to produce the reference biometric template. In this way, the relevant biometric technique is no more secure.

15 Moreover, the user authentication method according to the invention is also advantageous in case the authentication is mandatory for the access to an on-line service, in which the operator providing the service controls the data verification system 3. In  
20 fact, the operator offering the service can go on keeping the control over the verification of the users because, according to the invention, both data carrier 4 and data verification system 3 concur in performing the verification step in a secure way that cannot be  
25 repudiated (the non-repudiation of a session implies the impossibility for a user to negate having participated into the session itself).

Moreover, the global security provided by the user authentication method according to the invention is  
30 further increased by the fact that the creation logic of the reference biometric template 11 does not reside on the data carrier 4 but on the data enrolment system





TEL0903

19

2 that, preferably, is a separate system from the data verification system 3 and placed in a secure environment. On the data carrier 4 there are only the processing logic 5a that recomposes the reference  
5 biometric template and also performs the suitable cryptographic operations and the comparing logic 5b computing the correlation between reference biometric template and live template.

It is finally clear that to the herein described  
10 and shown user authentication method and its related architecture numerous modifications and variations can be made, all falling within the scope of the inventive concept, as defined in the enclosed claims.

For example, biometric techniques can be used that  
15 are different from face recognition, such as fingerprints, hand prints, voice templates, retinal images, calligraphic samples and the like.

Furthermore, the splitting algorithm used by the data enrolment system 2 can split the template  $t$  in  $n$   
20 portions, where  $n \geq 2$ , (e.g.,  $t_1, t_2, \dots, t_n$ ), with the property that it is impossible to obtain  $t$  from an arbitrary number  $i$  of its portions  $t_1, t_2, \dots, t_n$ , where  $i < n$ . In other words, only all the portions  $t_1, t_2, \dots, t_n$  combined together can recombine the original template  
25  $t$ . The size of the single portions can vary: depending on the chosen splitting algorithm they could not equal the size of the template  $t$ .

Moreover, the user authentication method according to the invention can be applied to different scenarios,  
30 such as for example:

- Stand Alone scenario, in which the user authentication method according to the invention is



used to protect the access to the data verification system 3 (ex. login to personal computer, palmtop, cellular phone-SIM) by a user provided with the data carrier 4;

5       - client-server scenario, in which the client scenario comprises the data carrier 4, preferably realised as a SIM-card, and a client portion of the data verification system 3, while the server scenario comprises a server portion of the data verification  
10 system 3. In particular, the server portion of the data verification system 3 can coincide or not with a central server (for example the server offering the required service). In this case, the client portion of the data verification system 3 can perform a more or  
15 less active role in the authentication process. For example, the client portion of the data verification system 3 can perform the function of detecting the biometric image of the user that has to be authenticated, then transferring it to the central  
20 server to which instead the live template generation is entrusted; the central server will then take care of transferring the live template to the client portion of the data verification system 3.

Alternatively, the client portion of the data  
25 verification system 3 can also generate the live template.

In both scenarios taken into account, the comparison operation between reference biometric template and live template is performed on the data  
30 carrier 4, then the recomposed reference biometric template never goes out of the data carrier 4. The result of this operation is then transferred in a



secure way (for example enciphered and signed) to the central server that decides whether granting or not the authorisation.

With reference to the client-server authentication  
5 scenario, if the central server plays an active role in the authentication process, the reference biometric template can be split, for example, in three portions:  $t_1$  stored on the data carrier 4,  $t_2$  stored on the central server 15, included in the server portion 3a of  
10 the data verification system 3, and  $t_3$  stored on the client portion 3b of the data verification system 3, as illustrated in figure 4. Alternatively, also the portion  $t_3$  of the reference biometric template can be stored on the server portion 3a. Interaction between  
15 all the systems is required for template recomposition and template verification.

According to the application's specific requirements, the configuration described above can also be extended to an arbitrary number of systems,  
20 each of them storing a respective portion of the splitted reference biometric template. In this case, an extended version of the previously described splitting algorithm can be used (see for example the book "Applied Cryptography" Second Edition, Chapter 3, pages  
25 70-71", author Bruce Schneier, published by John Wiley and Sons Inc).

Specifically, for  $n$  systems involved ( $n \geq 2$ ),  $n-1$  random strings are generated, at an enrolment step, having the same length of the original template  $t$ .  
30 These  $n-1$  random strings are then XORed with the template  $t$  for obtaining the  $n$ -th random string of the shared template. Each of these random strings is then



TEL0903

22

distributed to the respective system and the original template  $t$  is subsequently destroyed. At a verification step all these random strings should be present to recompose the original template  $t$ .

5        A further scenario including  $n$  systems, each of them storing a respective portion of the original template  $t$ , can require a template sharing scheme in which only  $m$  systems, with  $n > m \geq 2$ , are involved in the template recomposition and verification. A sharing  
10        scheme of this type is for example described in Shamir, *How to share a secret*, Communications of the ACM, 22 (1979), pp. 612-613.

More specifically, in this sharing scheme, called  $(m,n)$ - threshold scheme, the template  $t$  is divided into  
15         $n$  portions so that only  $m$  of them are needed to recompose the original template  $t$ . For example, as shown in figure 5, with a  $(3,4)$ - threshold scheme, the data enrolment system 2 can split the template  $t$  among the data carrier 4 ( $t_1$ ), the server portion 3a of the  
20        data verification system 3, comprising, for example, the central server 15 ( $t_2$ ) and a backup server 16 ( $t_4$ ) and the client portion 3b of the data verification system 3 ( $t_3$ ), so that only three of these systems are needed to recompose of the original template  $t$ . In this  
25        way, if the central server 15 is temporarily unavailable (or it has been compromised by an attack) the backup server 16 can replace it in the template recomposition.

The same security considerations, regarding the  
30        protection of the information exchanged between the systems involved in the template recomposition, are valid for the configurations described above, i.e. all





the template portions are digitally signed and enciphered, before transmission, using the appropriate private and public keys.

Further, in each one of the above described  
5 scenarios, all the communication channels between the systems are protected by means of public key cryptography methods like the ones previously described. Thus, all the request/response messages  
10 exchanged by the systems are signed and enciphered using the appropriate private and public keys. These messages can also include a nonce for protection against replay-attacks.

For increasing the privacy, the comparison operation between the reference biometric template and  
15 the live template is performed on the data carrier 4 but, depending on the specific application requirements, it can also be performed outside the data carrier 4, for example, by the data verification system  
3 (client portion or server portion).

20 Moreover, the Applicant outlines that biometric reference template splitting and its secure storing in the described distributed manner ensure increased resistance to template directed attacks and hence guarantees the privacy of the users..

25 Conventional security mechanisms (possibly based on the use of asymmetric cryptography) may also be used to guarantee the authenticity of the parties that take part to the secret sharing scheme and the confidentiality of the communication channels used.

30



24

# CLAIMS

1. User authentication method based on the use of identification biometric techniques comprising an  
5 enrolment step (20) and a verification step (40), said enrolment step (20) including the steps of:

- generating (22, 23) a reference biometric template from a first biometric image of a user to be authenticated;
- 10 - splitting (25) said reference biometric template into a first and a second reference biometric template portion;
- enciphering (27, 28) said first and second reference biometric template portion; and
- 15 - storing (29, 30, 31) each one of said reference biometric template portions into a different memory.

2. Method according to Claim 1, characterised in that said step of storing each one of said reference biometric template portions into a different memory  
20 comprises the step of:

- transmitting (29) said first reference biometric template portion from a first system (2) to a device (4), said first system (2) operating in said enrolment step (20);
- 25 - storing (30) said first reference biometric template portion into a memory (6) of said device (4), said device (4) operating in said verification step (40);
- transmitting (31) said second reference  
30 biometric template portion from said first system (2) to a second system (3), said second system (3) operating in said verification step (40); and



TEL0903

25

- storing (31) said second reference biometric template portion into a memory (11a) of said second system (3).

3. Method according to any one of Claims 1 or 2,  
5 characterised in that said verification step (40) comprises the steps of:

- generating (41, 42) a live template from a second biometric image of said user to be authenticated;

10 - enciphering (43) said live template; and

- transmitting (44) said live template and said second reference biometric template portion to said device (4).

4. Method according to Claim 3, characterised in  
15 that said verification step (40) comprises the steps of:

- deciphering (45, 47) said live template and said second reference biometric template portion;

- recomposing (46) said reference biometric  
20 template from said first and second reference biometric template portion; and

- comparing (48) said recomposed reference biometric template with said live template.

5. Method according to Claim 4, characterised in  
25 that said verification step (40) comprises the steps of:

- sending (49) a result of said comparison to said second system (3); and

- authenticating (50) or not authenticating said  
30 user depending on said result.

6. Method according to any one of Claims 2-5, characterised in that said step of splitting said



reference biometric template into a first and a second reference biometric template portion comprises the step of:

- destroying said biometric template performed by  
5 said first system (2).

7. Method according to any one of Claims 2-6, characterised in that said step of enciphering (27, 28) said first and second reference biometric template portion comprises the steps of:

- 10 - storing (21) a first and a second key ( $KE_{pub}$ ,  $KE_{pr}$ ) and a related digital certificate ( $C_2$ ) into a memory (7a) of said first system (2), said first and second keys ( $KE_{pub}$ ,  $KE_{pr}$ ) being respectively a public key ( $KE_{pub}$ ) and a private key ( $KE_{pr}$ ) associated with said  
15 first system (2);

- storing (21) a first and a second key ( $KU_{pub}$ ,  $KU_{pr}$ ) and a related digital certificate ( $C_4$ ) into said memory (6) of said device (4), said first and second keys ( $KU_{pub}$ ,  $KU_{pr}$ ) being respectively a public key ( $KU_{pub}$ )  
20 and a private key ( $KU_{pr}$ ) associated with said user to be authenticated;

- signing (27) said first and second reference biometric template portion with said private key ( $KE_{pr}$ ) of said first system (2); and

- 25 - enciphering (28) said first and second reference biometric template portion with said public key ( $KU_{pub}$ ) of said user to be authenticated.

8. Method according to any one of Claims 3-7, characterised in that said step of transmitting said  
30 live template and said second reference biometric template portion to said device (4) comprises the steps of:





- generating an aleatory value associated with the current data verification step (40), said aleatory value guaranteeing the authenticity of said current data verification step (40);

- 5       - signing and enciphering said aleatory value; and  
      - transmitting said aleatory value to said device (4).

9. Method according to Claims 7 or 8, characterised in that said step of enciphering said  
10 comparison biometric template comprises the steps of:

- storing a first and a second key ( $KV_{pub}$ ,  $KV_{pr}$ ) and a related digital certificate ( $C_v$ ) into said memory (11a) of said second system (3), said first and second keys ( $KV_{pub}$ ,  $KV_{pr}$ ) being respectively a public key ( $KV_{pub}$ )  
15 and a private key ( $KV_{pr}$ ) associated with said second system (3);

- signing (43) said live template with said private key ( $KV_{pr}$ ) of said second system (3); and

- enciphering (43) said live template with said  
20 public key ( $KU_{pub}$ ) of said user to be authenticated.

10. Method according to any one of Claims 8 or 9, characterised in that said step of deciphering said live template and said second reference biometric template portion comprises the steps of:

- 25       - deciphering the signature and the validity of said aleatory value;

- deciphering (45) said second reference biometric template portion with said private key ( $KU_{pr}$ ) of said user to be authenticated;

- 30       - verification its signature (45)

- deciphering (47) said live template with said private key ( $KU_{pr}$ ) of said user to be authenticated; and



TEL0903

28

- verification its signature (47).

11. Method according to any one of Claims 5-10, characterised in that said step of sending a result of said comparison to said second device (11) comprises  
5 the steps of:

- generating a message containing said result;
- enciphering said message.

12. Method according to any one of the previous claims, characterised in that said identification  
10 biometric techniques comprise at least one biometric identification technique of the type selected among: face recognition, fingerprints, hand prints, voice templates, retinal images, calligraphic samples.

13. Method according to any one of Claims 2-12,  
15 characterised in that said first and second system (2), (3) are respectively a data enrolment system and a data verification system and said device (4) is a data carrier.

14. Method according to Claim 1, characterised in  
20 that said step of splitting said reference biometric template includes the steps of

- splitting said reference biometric template into a plurality of reference biometric template portions, at least some of said reference biometric template  
25 portions being used to recompose said reference biometric template.

15. User authentication architecture bases on the use of biometric identification techniques comprising:

- at least one data enrolment system (2) for  
30 generating a reference biometric template from a first biometric image of a user to be authenticated, said data enrolment system (2) comprising a Host Computer



(7) to split said reference biometric template into a first and a second reference biometric template portion and for enciphering said first and second reference biometric template portion;

5 - at least one portable data carrier (4) associated with said user to be authenticated, said data carrier (4) comprising a memory (6a) for storing said first signed and enciphered reference biometric template portion; and

10 - at least one data verification system (3) comprising a memory (11a) for storing said second signed and enciphered reference biometric template portion.

16. Architecture according to Claim 15, characterised in that said data carrier (4) comprises a microprocessor (5) including a processing logic (5a) for deciphering said first and second reference biometric template portion, verification the signature and recomposing said reference biometric template from said first and second deciphered reference biometric template portion.

17. Architecture according to Claim 16, characterised in that said microprocessor (5) comprises a comparing logic (5b) to compare said recomposed reference biometric template with a live template generated by a second biometric image of the user to be authenticated, said second biometric image of the user to be authenticated being generated by the data verification system (3).

18. Portable data carrier (4) associated with a user that has to be authenticated through a user authentication architecture (1), said data carrier (4)



including a microprocessor (5) comprising a memory (6) for storing a first reference biometric template portion associated with said user to be authenticated, said first reference biometric template portion being  
5 signed and enciphered, said portable data carrier being adapted to receive as input, from said user authentication architecture, a second reference biometric template portion and a live template associated with said user to be authenticated, said  
10 second reference biometric template portion and said live template being signed and enciphered, said microprocessor (5) further comprising:

- a processing logic (5a) for deciphering said first and second reference biometric template portions  
15 and for recomposing therefrom said reference biometric template associated with said user to be authenticated;

- a comparing logic (5b) for comparing said reference biometric template recomposed with said live template and sending a result of said comparison to  
20 said user authentication architecture (1).

19. Data carrier according to Claim 18, characterised in that it comprises a substrate whose sizes are substantially rectangular.

20. Data carrier according to any one of Claims 18  
25 or 19, characterised in that said data carrier (4) is an access card or a credit card or a debit card or an identification card or a smart card or a SIM card.

21. Data verification system (3) comprising an electronic device (11) and a portable data carrier (4)  
30 associated with a user that has to be authenticated, said data carrier being adapted to store a first reference biometric template portion associated with a





user to be authenticated, said first reference biometric template portion being signed and enciphered;  
said electronic device comprising:

- a memory (11a) adapted to store a second  
5 reference biometric template portion associated with a user to be authenticated, complementary to said first portion, said second reference biometric template portion being signed and enciphered;
- an image acquiring and processing device (12)  
10 for generating a live template;  
said electronic device (11) being adapted to encipher and sign said live template, transmitting said second reference biometric template portion and said live template to said portable data carrier (4) and  
15 authenticating said user depending on the result of a comparison performed by said data carrier (4) between said live template and a reference biometric template of said user to be authenticated, said reference biometric template being rebuilt by using said first  
20 and second reference biometric template portion.22.  
Data verification system (3) comprising an electronic device (11) and a portable data carrier (4) associated with a user that has to be authenticated, said data carrier being adapted to store a first reference  
25 biometric template portion associated with a user to be authenticated, said first reference biometric template portion being signed and enciphered;

said electronic device comprising:

- a first memory (11a, 15) adapted to store a  
30 second reference biometric template portion associated with a user to be authenticated, said second reference biometric template portion being signed and enciphered;



TEL0903

32

- at least a second memory (11a, 15, 3b) adapted to store at least a third reference biometric template portion associated with a user to be authenticated, said third reference biometric template portion being signed and enciphered, wherein said first, second and at least third reference biometric template portions are such that the reference biometric template can be recomposed from a subset of at least two of said reference biometric template portions;
- 10 - an image acquiring and processing device (12) for generating a live template;
- said electronic device (11) being adapted to encipher and sign said live template, transmitting said second reference biometric template portion and said live template to said portable data carrier (4) and authenticating said user depending on the result of a comparison performed by said data carrier (4) between said live template and a reference biometric template of said user to be authenticated, said reference biometric template being rebuilt by using said first and second reference biometric template portion.

23. Program for electronic processor that can be loaded into the memory of at least one electronic processor and including program codes for performing the steps of the method according to any one of Claims 1-14 when said program is executed by said electronic processor.



## ABSTRACT

The present invention refers to a user authentication method based on the use of 5 identification biometric techniques comprising the steps of:

- generating a reference biometric template from a first biometric image of a user to be authenticated;
- splitting the reference biometric template into 10 a first and a second reference biometric template portion that can be physically separated;
- signing and enciphering the first and the second reference biometric template portion;
- storing the signed and enciphered first and the 15 second reference biometric template portion into different memories.

(Fig.1)



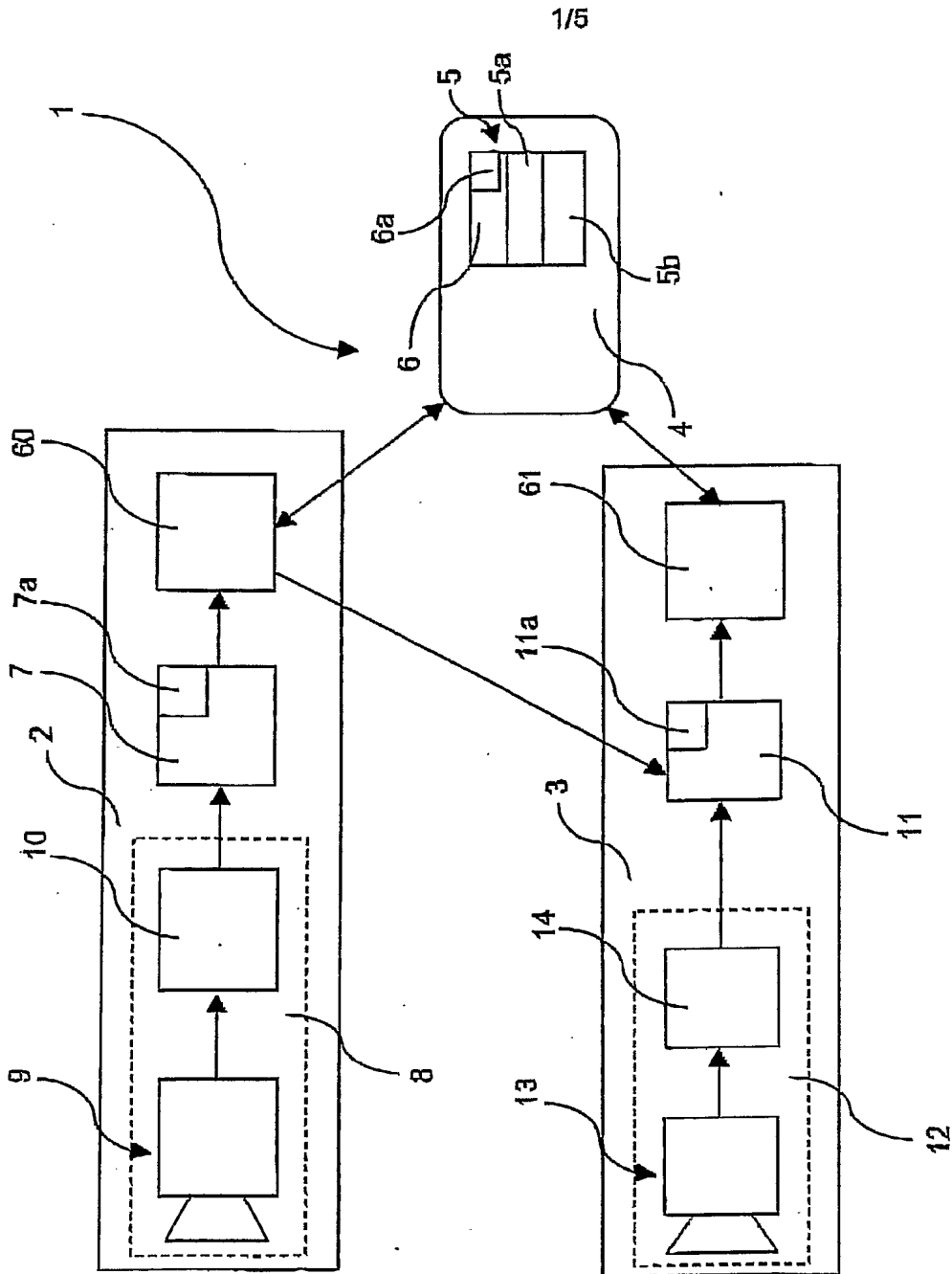


FIG. 1





2/5

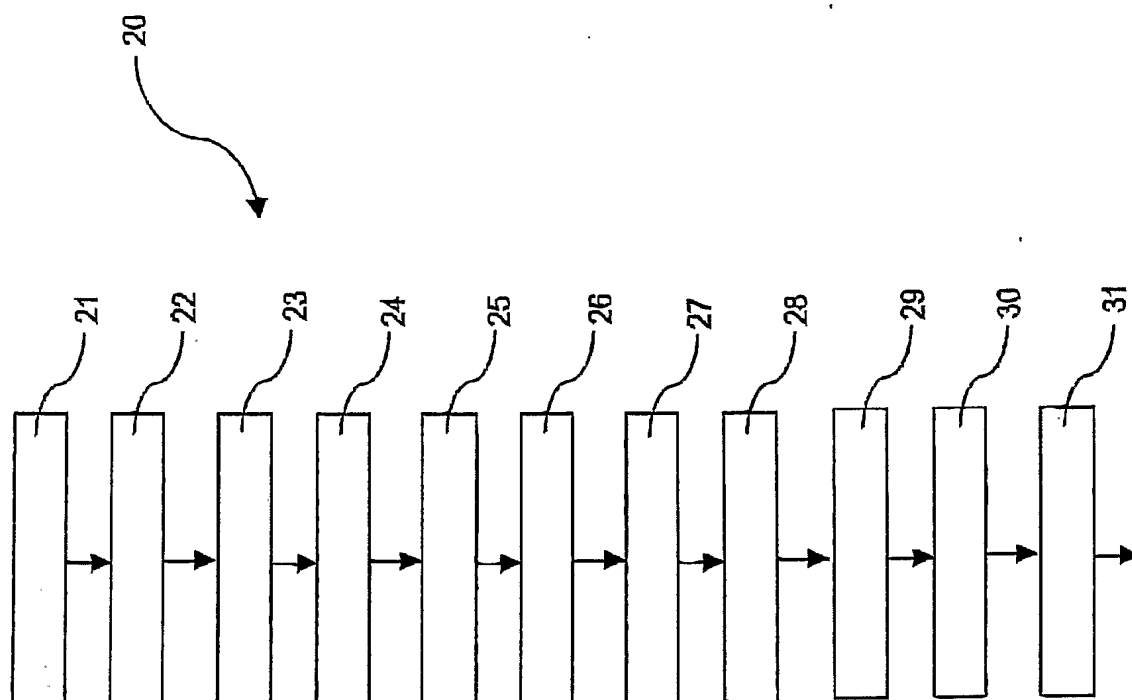


FIG. 2



3/5

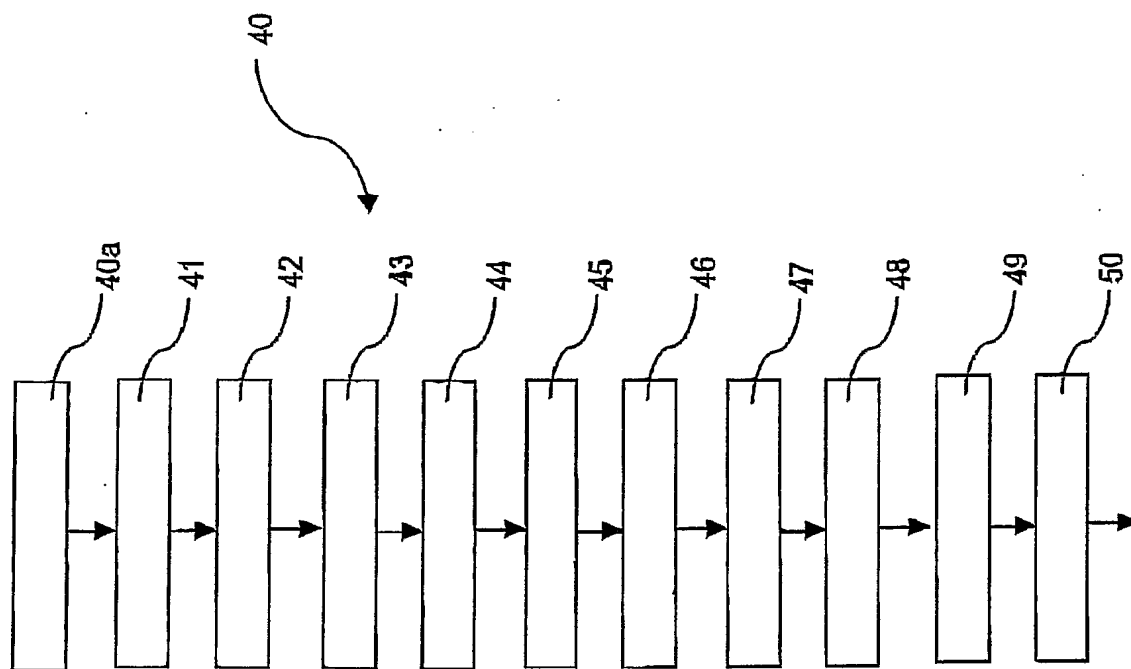


FIG.3



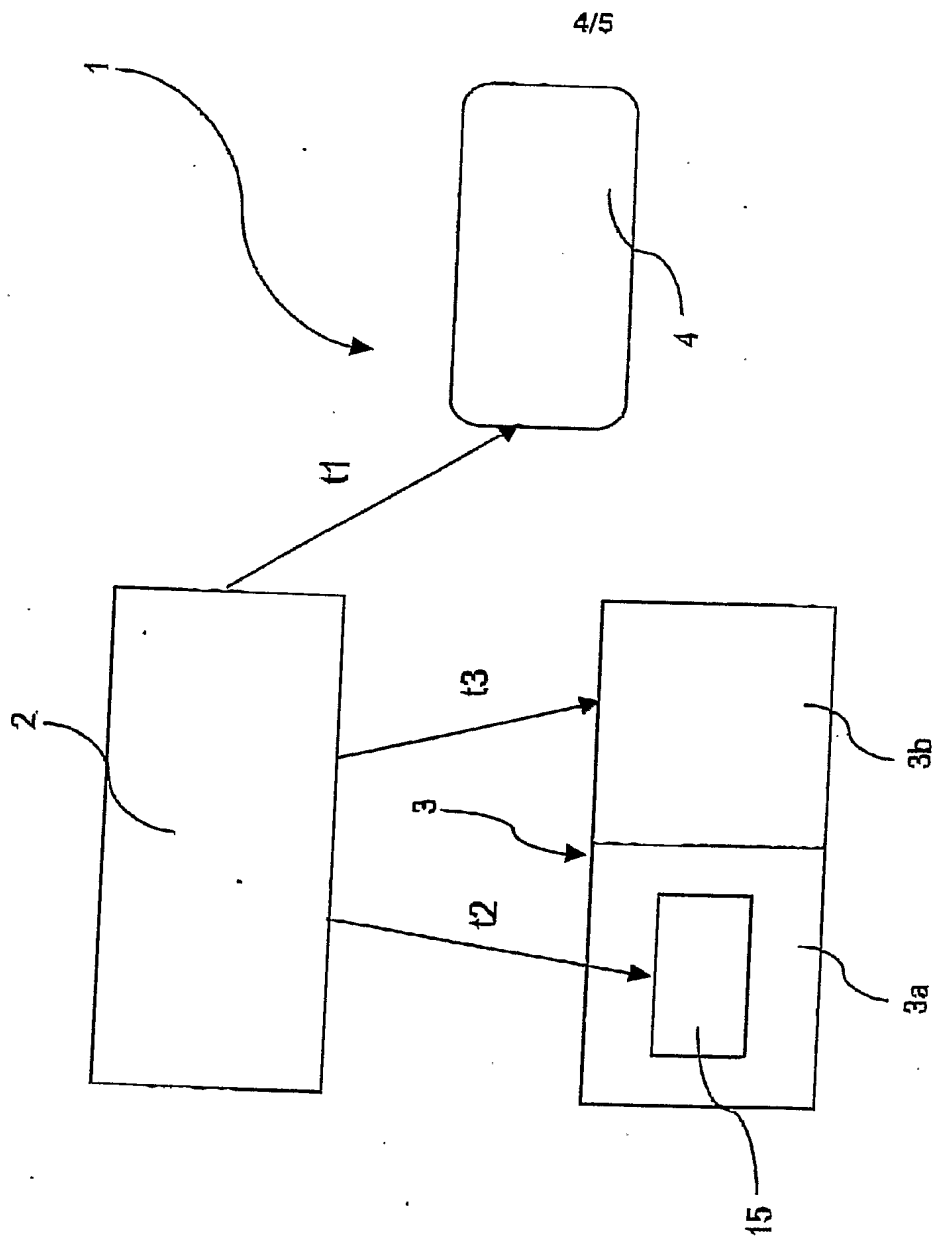


FIG. 4



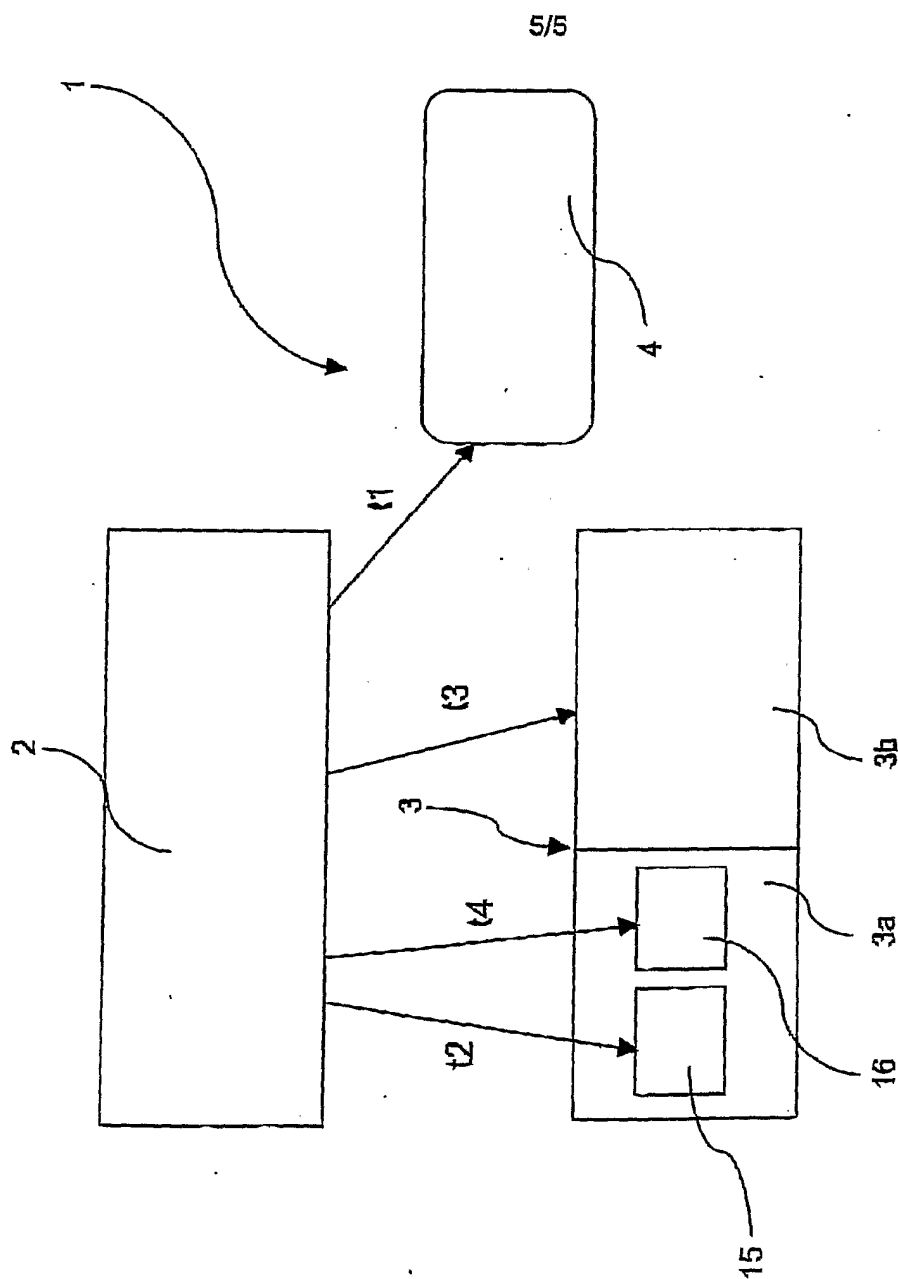


FIG. 5



